CLAIMS

What is claimed is:

1. A system for conducting a transaction via a network, comprising:

a first site coupled to a network;

a terminal coupled to the network for performing a first portion of a transaction with the first site via the network;

a second site coupled to the network for performing a second portion of the transaction that requires personal data, wherein the second site transmits to the terminal via the network a certificate for verifying the identity of the second site;

a secure device coupled to the terminal, the secure device containing an encrypted version of the personal data and a first key for decrypting the encrypted personal data, wherein the secure device provides the terminal with the encrypted personal data and the first key to the terminal;

the terminal having logic for decrypting the encrypted personal data using the first key, logic for re-encrypting the decrypted personal data with a second key, and logic for transmitting the re-encrypted personal data to the second site via the network; and

the second site having logic for decrypting the re-encrypted personal data and logic for using the personal data to complete the second portion of the transaction.

2. The system of claim 1, wherein the secure device includes a special region that, if tampered with, renders the secure device inoperable and thereby prevent access to the first key contained therein.

3. The system of claim 1, wherein communications between the terminal and the secure device and between the terminal and the second site are encrypted with one or more symmetric keys.

4. The system of claim 1, wherein the personal data includes at least one of credit card information and credit history information.

5. The system of claim 1, wherein a list containing information for authenticating the certificate of the second site is transmitted from the first site to the terminal via the network prior to receipt of the certificate by the terminal.

6. The system of claim 1, wherein the transaction comprises a commercial transaction and the first site comprises an e-commerce site.

7. The system of claim 1, wherein the secure device provides the terminal with the encrypted personal data prior to and separately from the first key.

8. The system of claim 1, wherein the second key comprises a public key associated with the second site.

9. The system of claim 1, wherein a second certificate associated with the terminal is provided to the secure device to authenticate the terminal before the secure device provides the terminal with the encrypted personal data and first key.

10. The system of claim 1, wherein a notification is transmitted from the second site to the first site via the network upon completion of the second portion of the transaction.

11. The system of claim 1, wherein the secure device is detachably coupled to the terminal.

12. A method for conducting a transaction via a network, comprising the steps of:

receiving, via a network, a request from a site to perform a portion of a transaction with a terminal coupled to the network, wherein an initial portion of the transaction is performed between the site and the terminal via the network, wherein personal data about a user of the terminal is required to complete the requested portion of the transaction;

transmitting a certificate to the terminal via the network, wherein the terminal authenticates the certificate and transmits via the network an indication that indicates that the certificate has been authenticated;

transmitting a request for the personal data to the terminal via the network, wherein a secure device is coupled to the terminal, wherein the secure device contains an encrypted version of the personal data and a first key for decrypting the encrypted personal data, wherein the second device provides the terminal with the encrypted personal data and the first key and the terminal uses the first key to decrypt the encrypted personal data;

providing the terminal with a second key via the network, wherein the terminal re-encrypts the personal data with the second key;

receiving the re-encrypted personal data from the terminal via the network;

decrypting the re-encrypted personal data with the second key; and

completing the requested portion of the transaction using the personal data.

13. The method of claim 12, wherein the secure device includes a special region that, if tampered with, renders the secure device inoperable and thereby prevent access to the first key contained therein.

14. The method of claim 12, wherein communications with the secure device and the terminal are encrypted with one or more symmetric keys.

15. The method of claim 12, wherein the personal data includes at least one of credit card information and credit history information.

16. The method of claim 12, wherein, prior to transmission of the certificate to the terminal, the site transmits to the terminal via the network a list containing information for authenticating the certificate.

17. The method of claim 12, wherein the secure device provides the terminal with the encrypted personal data prior to and separately from the first key.

18. The method of claim 12, wherein a second certificate associated with the terminal is provided to the secure device to authenticate the terminal before the secure device provides the terminal with the encrypted personal data and first key.

19. The method of claim 12, further comprising notifying the site via the network of the completion of the requested portion of the transaction.

20. A computer program product for conducting a transaction via a network, comprising the steps of:

computer code for performing a first portion of transaction with a first site via a network, wherein the first site contacts a second site via the network to request that the second site perform a second portion of the transaction, wherein personal data about a user is required to complete the second portion of the transaction;

computer code for receiving a certificate from the second site via the network;

computer code for authenticating the certificate of the second site;

computer code for contacting the second site via the network if the certificate is authenticated;

computer code for receiving a request for the personal data from the second site via the network;

computer code for requesting the personal data from a secure device, wherein the secure device contains an encrypted version of the personal data and a first key for decrypting the encrypted personal data;

computer code for receiving the encrypted personal data and the first key from the secure device;

computer code for decrypting the encrypted personal data using the first key;

computer code for re-encrypting the personal data using a second key associated with the second site; and

computer code for transmitting the re-encrypted personal data to the second site via the network, wherein the second site decrypts the re-encrypted personal data with the second key and uses the personal data to complete the second portion of the transaction.